REMARKS

In response to the Office Action dated February 16, 2011, Applicants respectfully request reconsideration and withdrawal of the rejections of the claims.

Claims 18-20 were rejected under the first paragraph of 35 U.S.C. § 112. The Office Action states that there is no written description in the specification of the concept of decrypting, by a secure electronic device, an encrypted IMEI that is received from a storage support module, using a second key. To remove the basis for this ground of rejection, claims 18, 19 and 20 have been amended to delete the recitations that pertain to encryption of the IMEI using a first key, and decryption of the IMEI using a second key. The references to authentication of the IMEI, which were previously added by amendment, have also been removed from these claims.

It is respectfully submitted that the amendments to claims 18-20 do not raise any new issues that require further consideration or search. Rather, the nature of these amendments is to delete recitations that were previously added by amendment, and thereby remove the basis for the rejection under the first paragraph of 35 U.S.C. §112. It is respectfully submitted that the patentability of the subject matter defined in the presently amended claims has been previously considered by the Examiner. Accordingly, entry of the amendments is submitted to be proper since, at a minimum, they reduce issues for appeal.

Claims 2, 4-7, 9, 11-16 and 18-20 were rejected under 35 U.S.C. § 103, on the basis of the Simmons Patent Application Publication (US 2004/0043792) in view of the Portalier et al. patent (GB 2 355 892). Claims 10 and 17 were rejected on the basis of these two references, in further view of the state of the art described in the background portion of the present application. For the reasons discussed hereinafter, it is respectfully submitted that the Simmons and Portalier references, whether considered individually or in combination, do not suggest the features of the pending claims to a person of ordinary skill in the art.

As discussed in the background portion of the application, a problem that has arisen in the mobile telephone industry is the theft of handsets. In an effort to thwart the reuse of stolen handsets, the unique identifier of a stolen handset, namely its International Mobile Equipment Identity (IMEI), is placed on a black list. When a handset is used on a mobile network, its IMEI is transmitted to the network operator. By checking a received IMEI against the black list, the network operator can block the use of handsets which have been reported to be stolen.

However, as noted on page 2 of the specification, it has become fairly easy to get around the hurdles of a black list, by modifying the IMEI of a handset. To this end, in more recently manufactured handsets, the IMEI is stored in a memory that inhibits physical modification of the IMEI, such as a PROM.

However, even this further effort to inhibit the use of stolen handsets is not totally successful. As noted in the last paragraph on page 2 of the specification, if a fraudulent operating system is implemented on the handset, it may modify the IMEI that is retrieved from the physically secure memory before sending it on to the network, and thus avoid the black list prohibition.

The claimed subject matter addresses this latter concern, to inhibit rogue software within the handset from modifying the IMEI as it is being transferred from the physically secure memory to the network. In accordance with the claimed invention, a secure electronic module, e.g. a SIM card within the mobile handset, authenticates a storage module that stores the IMEI. Once the storage module has been authenticated, a secure communication channel is established between the storage module and the secure electronic module. For instance, Figure 1 of the present application illustrates an example of a handset 1 having a storage support 2, e.g. PROM, and a secure module 31, e.g. SIM card, housed in a connector 3. The secure communication channel between the PROM 2 and the SIM card 31 is represented by reference number 6.

This secure communication channel is used to transmit the IMEI from the storage module to the secure electronic module, to thereby enable the handset to access the mobile communication network. Thus, by establishing this secure communication channel between the storage module and the secure electronic module, and using this secure channel for the transfer of the IMEI, any fraudulent software that may be resident on the handset is inhibited from modifying the IMEI during the transfer.

It is respectfully submitted that the cited references do not suggest the claimed features to a person of ordinary skill in the art. In particular, neither of the references discloses the concept of authenticating a module that stores an IMEI by a secure electronic module, nor establishing a secure communication channel between the storage module and the secure electronic module. Consequently, any logical combination of the teachings of the references likewise would not suggest these claimed features to a person of ordinary skill in the art.

Claim 18 recites a telephone handset comprising, among other elements, a storage support module storing an IMEI, and a secure electronic module. Insofar as it is relevant to the claimed subject matter, the Simmons reference discloses a mobile equipment (ME) 10 that includes a user identity module (SIM) 20 and an IMEI unit 15 (see paragraph 0028).

Claim 18 goes on to recite that the handset includes a memory containing program instructions that control the handset to "authenticate, by the secure electronic module, the storage support module". The Office Action asserts that the Simmons reference discloses this claimed feature, citing paragraph 0030 on page 3 of the reference. This paragraph merely repeats the information described above in connection with paragraph 0028 of the reference, namely that the mobile equipment 10 contains a SIM 20 and also contains the IMEI unit 15. It does not, however, disclose that the SIM 20 authenticates the IMEI unit 15. In fact, the reference does not describe any form of communication or relationship between the SIM 20 and the IMEI unit 15, except that they are individual components of the mobile equipment 10.

Claim 18 further recites that, in the event the secure electronic module determines that the storage support module is authentic, a secure communication channel is established "between the storage support module and the secure electronic module". With reference to this claimed feature, the Office Action asserts that it is described in the Simmons reference at paragraphs 0042 and 0049. Turning first to paragraph 0042, it pertains to the procedure by which the SIM card 20 authenticates the mobile station 10, which is described in greater detail in paragraph 0039. As stated therein, a unique challenge is "initiated by the SIM card 20 to externally verify that the terminal device is compatible with pre-paid operation by generating a random number and sending it to the ME 10 …"

Thus, the Simmons reference discloses that the SIM card authenticates the mobile terminal. It does not, however, disclose that the SIM card authenticates the

IMEI unit 15 itself. As such, it does not provide a solution to the problem addressed by the claimed invention. In particular, even if the terminal, as a whole, is authenticated, the possibility still exists that fraudulent software could be resident within the terminal that modifies the IMEI after it is read out of the unit 15 and before it is provided to the SIM card 20. In other words, the authentication of the mobile terminal 10 does not inherently establish a secure communication channel between the IMEI unit 15 and the SIM card 20. As noted previously, the Simmons reference does not describe any communications between the IMEI unit 15 and the SIM card 20, let alone that such communications take place over a secure channel.

Paragraph 0049 of the Simmons reference pertains to an optional feature that has nothing to do with secure communications. Normally, a portable SIM card is capable of being used with various telephone handsets, each of which has its own unique IMEI. See the last sentence of paragraph 0049. The earlier portion of the paragraph describes an option by which the SIM card can be bound to one particular handset. Under this option, the first time that the SIM card presents a challenge to the handset to authenticate it, the IMEI of the handset can be stored in read only memory of the SIM. Thereafter, the SIM will only operate with that particular handset, i.e. the one having the IMEI stored in the SIM card's memory. This paragraph does not provide any indication of how the IMEI, or other identifying information, is provided to the SIM card. In particular, it does not disclose that the information is provided by means of a secure communications channel that is established between the SIM card and the IMEI unit 15.

Accordingly, it is respectfully submitted that the Simmons patent does not disclose either of the two above-discussed claim elements. At best, the Simmons reference discloses that the SIM card functions to authenticate the mobile terminal. It does not, however, disclose, nor otherwise suggest, that the SIM card authenticates the IMEI unit 15. As discussed above, authentication of the mobile terminal, as a whole, is not the same as, nor does it provide the same result as, authentication of the specific memory unit that stores the IMEI. Nor does it disclose a secure communication channel between the SIM card 20 and the IMEI unit 15.

The Portalier reference does not overcome these distinctions between the Simmons publication and the claimed subject matter. In relevant part, it discloses a particular technique for implementing the above-noted option of the Simmons reference, namely to bind a SIM card to a particular handset. Referring to the discussion that begins at page 2, line 22, the Portalier reference discloses that this result can be accomplished by duplicating the identity code of the SIM card (IMSI) in the memory of the mobile telephone. Subsequently, when an attempt is made to use the mobile telephone, if the code stored in the phone does not match that of the SIM card, operation of the phone is blocked.

In rejecting the claims, the Office Action refers to page 3, lines21-26 of the Portalier reference, and asserts that this passage discloses an encrypted communication channel between one data storage device and another storage device. It is respectfully submitted that the reference does not support this assertion. Rather, it discloses that a preferred way to perform the binding of the SIM card to the phone is to couple the IMSI code of the card with the IMEI code of the phone. This coupling results in the production of a new code that is stored in the memory of the phone. See, for instance, page 6, lines 8-15.

The Portalier reference does not disclose that, as part of this process, the SIM card 13 authenticates the memory module 10 in which the IMEI of the phone is stored. Nor does it disclose that a secure communication channel is established on the basis of such authentication, via which the IMEI is transferred to the SIM card.

A logical combination of the teachings of the Simmons and Portalier references would be to bind a SIM card to a particular phone according to the technique disclosed in the Portalier patent, in order to implement the option disclosed in paragraph 0049 of the Simmons publication. Such a combination does not result in the claimed subject matter. In particular, neither reference discloses (1) authenticating a storage module of the handset, in which its IMEI is stored, by the secure electronic module, e.g. SIM card, nor (2) establishing a secure communication channel between the storage module and the SIM card on the basis of such authentication. Consequently, any logical combination of their teachings likewise would not suggest these claimed features to a person of skill in the art.

At best, the Simmons publication discloses the authentication of a mobile terminal by a secure electronic module such as a SIM card. It does not disclose authentication of a storage module, per se, within the mobile terminal. Moreover, even if the authentication of the mobile terminal was interpreted to encompass authentication of the storage module, to which Applicants do not acquiesce, there is still no suggestion to establish a secure communication channel between the storage module, on one hand, and the secure electronic module, on the other hand, on the basis of such an authentication, i.e. “in the event that the secure electronic module determines that the storage support module is authentic”, as recited in claims 18-20.

In conclusion, it is respectfully submitted that the combined teachings of the references do not suggest the claimed subject matter to a person of ordinary skill in the art, and that all pending claims are therefore patentably distinct from the Simmons and Portalier references, whether they are considered individually or in any logical combination thereof. Reconsideration and withdrawal of the rejections and allowance of all pending claims is respectfully requested.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: June 16, 2011

By: /James A LaBarre/
James A. LaBarre
Registration No. 28632

Customer No. 21839
703 836 6620